-11-

stored in another location in each software product, and each of those another locations is different in different software products so that it would not be discovered and altered. And, each such software product, when executed, will automatically check the unencrypted identity stored therein against the decryption result of the encrypted one, if they are not consistent, the software product will fail to operate. The identity or encrypted identity of the rightful user being included into each of the software products by the central computer at the time when the central computer is to supply the same to the user computer. Further, to prevent the AS sub-program from mistakenly regarding a software product which stored in the computer and which being not supplied from the central computer, as a software product under its control, the central computer may further include information in a third predetermined location of each software product for indicating this fact, that is, the software product being supplied from the central computer, to the AS sub-program and each software product will not operate if when being executed, it finds that information therein being altered.

It should be noted that the above embodiments are given by way of example only, and it will be obvious to those skilled in the art that various changes and modifications may be made without departing from the spirit of the present invention.

-13-

What is claimed is :

1.(Second time Amended) <u>A method for protecting software from unauthorised use</u> , <u>comprising the steps of</u> :

[Authorising software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said authorising software being for, when executed, 1] permitting use of said software desired to be protected on said computer : 2]]

determining the existence of <u>an</u> identity [software in a memory] means <u>in</u> <u>association with a computing means</u> [under control of said computer] ;

<u>using a favourable result of said determination of existence as a pre-condition</u> <u>for permitting use of said software desired to be protected on said computing means</u> ;

<u>wherein</u> said identity [software] <u>means</u> being for

[use on said computer to provide information of said rightful or authorised user ;]

[said information being essentially used in]

enabling <u>electronic money transfer</u> operation(s) for which [said] <u>a</u> rightful [or authorised] user <u>of said software desired to be</u> protected has to be responsible ;

<u>wherein said rightful user being a user who has already obtained a right of</u> <u>using said software desired to be protected, with any necessary payment therefor,</u> <u>being made ; and the use of said software desired to be protected is being permitted</u> <u>without a said operation being performed</u>.

[and the existence of said identity software in a memory means under control of said computer is being determined without a said operation being performed by said remote computer]

[wherein use of said software desired to be protected on said computer will not be permitted if said identity software is determined as being not existing in a memory means under control of said computer .]

-14-

2. (First time Amended) <u>A method for protecting software from unauthorised use</u> , <u>further comprising the steps of</u> :

[Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1, wherein further comprising software, when being executed, for]

authenticating said identity software ; [and if the result of the authentication of said identity software is unfavourable,]

said identity software will [further] be determined as [not] existing in [a] <u>said</u> memory means [under control of said computer], <u>if the result of said authentication is favourable and as not existing if otherwise</u> .

4. (First time Amended) <u>A method for protecting software from unauthorised use</u> , [Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1,]

wherein said operation being operation related to making payment from an account of said rightful [or authorised] user.

5. (First time Amended) <u>A method for protecting software from unauthorised use</u> , [Authorising software, stored in a device or existing physically on a medium, as claimed in claim 1,]

wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

-15-

6. (First time Amended) <u>A method for protecting software from unauthorised use</u> , [Authorising software, stored in a device or existing physically on a medium, as claimed in claim 5,]

wherein further comprising an encrypted identity of its rightful user ; and if one of said protected programs stored in said computer has a valid user identity which being not consistent with the decryption result of said encrypted identity in said authorising software, said authorising software will not permit use of said protected programs .

7. (Second time Amended) Protection software for use on a [computer] <u>computing device</u>, to protect [purchased computer] software <u>against unauthorised use</u> [by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof] ;

said protection software comprising :

identity software [for use on said computer to provide information of said rightful or authorised user ;]

[said information] being [esentially] <u>essentially</u> used <u>on said computing device</u> in enabling operation(s) for which [said] <u>a</u> rightful [or authorised] user <u>of said software desired to be protected</u> has to be responsible ;

authorising software <u>effectively under the control of said rightful user</u> for, when executed, permitting use of said software desired to be protected, on said [computer] <u>computing device</u> ;

Wherein said identity software and said authorising software are contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually.

-16-

8. (First time Amended) Protection software [, stored in a device or existing physically on a medium,] as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful [or authorised] user.

9. (First time Amended) Protection software [, stored in a device or existing physically on a medium,] as claimed in claim 7, wherein said authorising software [includes] contains said identity software.

10. (Second time Amended) Authorising program for use on a [computer] computing device, to protect other [computer] software against unauthorised use [by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof] ;

said authorising program being effectively under the control of a rightful user of said software desired to be protected for, when executed, permitting use of said software desired to be protected on said [computer] computing device ;

wherein information [of] related to said rightful [or authorised] user of said software desired to be protected, exists in said authorising program and being accessible to the user thereof ;

said information being essentially used on said computing device in enabling operation(s) for which said rightful [or authorised] user has to be responsible .

-17-

11. (First time Amended) Authorising program [, stored in a device or existing physically on a medium,] as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful [or authorised] user.

12. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Protection software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said protection software comprising :]

obtaining a first information from a user of a computing device storing an identity software ;

using said first information received being correct as a pre-condition for permitting use of said software desired to be protected on said computing device ;

wherein said identity software being for [, with password protection against used by unauthorised user,] providing a second information [of said] related to the rightful [or authorised] user of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

and said second information being essentially used in enabling electronic money transfer operation(s) for which said rightful [or authorised] user has to be responsible ;

wherein said rightful user being a user who has already obtained a right of using said software desired to be protected, with any necessary payment therefor, being made ; and the use of said software desired to be protected is being permitted without a said operation being performed.

-18-

[authorising software for, when executed, permitting use of said software desired to be protected on said computer ;]

[wherein use of said software desired to be protected will not be permitted if a correct password not entered by user .]

13. (First time Amended) Authorising program [, stored in a device or existing physically on a medium,] as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful [or authorised] user.

14. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[Authorising software for use on a computer to protect other computer software by discouraging a rightful or authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof ;]

[said authorising software being for, when executed, 1) permitting use of said software desired to be protected on said computer ; 2)]

authenticating identity [software] information existing in a memory means [under control of said computer] associated with said computing means ;

using a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said computing means ;

wherein said identity [software being for use on said computer to provide information of said rightful or authorised user ;]

[said] information being essentially used on said computing means in enabling *electronic money transfer* operation(s) for which [said] a rightful [or authorised] user of said software desired to be protected has to be responsible ;

-19-

wherein said rightful user being a user who has already obtained a right of using said software desired to be protected, with any necessary payment therefor, being made ; and the use of said software desired to be protected is being permitted without a said operation being performed.

[wherein use of said software desired to be protected will not be permitted if the result of said authentication of said identity software is not favourable .]

15. (First time Amended) Authorising program [, stored in a device or existing physically on a medium,] as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful [or authorised] user.

16. (First time Amended) A method for protecting software distributed by a vendor from unauthorised use , comprising the steps of :

obtaining by an installing software running on a computing device , first information from a user ;

determining, by said installing software, from said computing device second information related to the hardware or/and software thereof , if said first information received being confidential information of a rightful user of said software desired to be protected ;

thereafter, determining by said installing software, from the computing device onwhich said installing software runs, third information related to the hardware or/and software thereof;

-20-

determining , by said installing software, if said third information is consistent with said second information ;

using, by said installing software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the computing device onwhich said installing software runs;

wherein said installing software being supplied from said vendor to said rightful user.

[Protection software for use on a computer, to protect other computer software by discouraging a rightful or an authorised user thereof from enabling or allowing other person(s) to use said software desired to be protected or a duplication copy thereof;

said protection software comprising :

identity software for, with protection against used by unauthorised user, providing information of said rightful or authorised user ;

said information being in enabling operation(s) for which said rightful or authorised user has to be responsible ;

authorising software for, when executed, permitting use of said software desired to be protected on said computer ;

wherein use of said software desired to be protected will not be permitted if said protected identity software is not being caused to be usable by correct information obtained from user .]

17. A method for protecting software from unauthorised use, comprising the steps of :

a)   determining, the existence of an identity software/means which being essential used in a computing device, say, first computing device, for accessing a remote electronic transaction system an account of a rightful user of said software desired to be protected, in said computing device ✗, *by an installing software;*

b)   establishing a communication between said computing device and a computing means of said remote electronic transaction system, for verifying said account is a valid account ;

-21-

c)   using by ~~and~~ *said* installing software running on said computing device, a favourable result of said determination of existence and verification as pre-conditions for determining from said computing device first information related to the hardware or/and software thereof;

thereafter, determining by said installing software, from the computing device onwhich said installing software runs, say, second computing device, second information related to the hardware or/and software thereof;

determining , by said installing software, if said first information is consistent with said second information;

if the result of said determination of consistence is not favourable, repeat steps a) to c) with said second computing device ; otherwise, using by said installing software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on said second computing device ;

wherein said rightful user being a user who has already obtained a right of using said software desired to be protected on any suitable computing devices, with any necessary payment therefor, being made ; *and said installing software being specific to, said rightful user.*

18. A method for protecting software *distributed by a vendor* from unauthorised use, comprising the steps of :

using, an installing software running on a computing device, "the existence of an identity software/means which being ~~essential~~ *essentially* used in said computing device for enabling operation(s) for which a rightful user of said software desired to be protected has to be responsible, in said computing device" ; as a pre-condition for determining from said computing device first information related to the hardware or/and software thereof . without causing a said operation to-be performed ;

being

electronic money Transfer

-22-

thereafter, determining by said installing software, from the computing device onwhich said installing software runs, second information related to the hardware or/and software thereof;

determining , by said installing software, if said first information is consistent with said second information ;

using by said installing software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the computing device onwhich said installing software runs .

without causing a said operation being performed.

Claims 17, 18 are new claims